IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,

Plaintiff,

8:17CR289

VS.

FINDINGS AND RECOMMENDATION

MARK RINGLAND,

Defendant.

This matter is before the Court on the Motion to Suppress Evidence and Statements and Request for Evidentiary Hearing (Filing No. 47) and the Motion to Suppress, Application for *Franks* Hearing, and Request for Evidentiary Hearing and Oral Argument (Filing No. 49) filed by Defendant, Mark Ringland. Defendant filed briefs in support of both motions (Filing No. 48; Filing No. 50) and the government filed a brief in opposition (Filing No. 58).

The Court held an evidentiary hearing on Defendant's motions on July 19, 2018, and a transcript (TR.) of the hearing was prepared and filed on August 4, 2018. (Filing No. 68). Defendant was present with his attorney, Richard McWilliams. The government was represented by Assistant United States Attorney, Michael Norris. Mark Dishaw ("Deputy Dishaw"), a Deputy with the Douglas County Sheriff's Office and an assigned Investigator to the FBI Child Exploitation Task Force, testified on behalf of the government. The Court received into evidence, without objection, Exhibit 1 (Declaration of John Shehan) and Exhibit 2 (DVD of seven (7) CyberTipline Reports) offered by the government, and Exhibits 101-163 offered by Defendant. (TR. 6, 56). Exhibits 101-108, 111-121, and 128-143 constitute thirty-five CyberTipline reports. Exhibits 109-110, 122-123, 124-125, and 126-127 constitute the four separate applications and warrants relevant to Defendant's motions.

The Court granted Defendant's oral request to file supplemental briefing following the evidentiary hearing; Defendant filed a supplemental brief on August 10, 2018, (<u>Filing No. 70</u>) and the government filed a supplemental brief on August 30, 2018, (<u>Filing No. 73</u>). The government's supplemental brief incorporates two attachments marked as "Exhibit 1" (<u>Filing No. 73-1</u> -

Google's Terms of Service) and "Exhibit 2" (Filing No. 73-2 - Declaration of Cathy A. McGoff). This matter is now fully submitted to the Court. For the following reasons, the undersigned magistrate judge recommends that Defendant's motions be denied.

BACKGROUND

Defendant is charged in a two-count Indictment with receipt of child pornography and possession of child pornography under 18 U.S.C. §§ 2252(a)(2), (a)(4)(B) and (b)(2). (Filing No. 20). Investigator C.J. Alberico ("Investigator Alberico") of the Nebraska State Patrol prepared a report (Exhibit 163) that "provides a pretty succinct timeline" of her investigation leading up to the charges being filed in this case. (TR. 55; Ex. 163). According to Investigator Alberico's report, Google, Inc. ("Google") first provided information to the National Center for Missing and Exploited Children ("NCMEC") that a user of Google's services "had uploaded over seven hundred (700) files suspected of depicting sexually explicit conduct involving a minor." Google identified the user by email address, mringland69@gmail.com, with associated telephone number 402-***-0642.² Several IP addresses were associated with the uploaded files, which NCMEC traced to Sprint PCS in Omaha, Nebraska. Based on this information, on April 17, 2017, NCMEC created seven CyberTipline Reports: #19083866, #19153972, #19938982, #19986242, #20035870, #20260729 and #20293287. (Ex. 163 at p. 1). Exhibit 2 includes these seven CyberTipline Reports containing the 502 images viewed by Investigator Alberico. (TR. 10). On May 12, 2017, Investigator Alberico submitted a preservation letter to Google for the email account mringland69@gmail.com. (Ex. 163 at p. 1).

Deputy Dishaw explained the general process of how CyberTipline reports are generated and provided to law enforcement. Deputy Dishaw testified that electronic service providers ("ESP") such as Google have proprietary methods to filter and identify known child pornography images based on hash values. (TR. 21-22, 24-25,51-53). The ESP will then view the file images and report potential violations to NCMEC, and then NCMEC will generate CyberTipline reports

¹ To avoid confusing these post-hearing exhibits with Exhibits 1 and 2 received at the evidentiary hearing, hereinafter, the post-hearing exhibits will be referred to by their filing numbers. The government requested that the evidentiary record remain open until all briefs were submitted, without objection, although the parties later agreed that a motion would be filed to reopen the record for the Court's consideration. (TR. 11, 57-58, 69).

² On May 16, 2017, Investigator Alberico served a subpoena on Sprint to identify the subscriber information associated with telephone number 402-***-0642. Sprint identified the subscriber as "H. L.," residing at an address in Carter Lake, Iowa. Investigator Alberico's investigation ultimately did not link H.L. to this case. (Ex. 163 at p. 1).

to send to law enforcement. (TR. 14-16). Deputy Dishaw testified that, particularly after the ruling in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), investigators make sure that they are only reviewing files that the ESP reviewed first and reported to NCMEC. (TR. 16-17, 25-26, 52-53). Deputy Dishaw explained that if NCMEC is not clear whether the ESP reviewed a file, NCMEC will make a notation for the investigator, and then the investigator will contact the ESP to confirm whether or not the ESP viewed the file. Deputy Dishaw testified that if the ESP confirms it did not view the file, he will obtain a search warrant to view those files. (TR. 18).

Investigator Alberico continued to receive additional CyberTipline reports subsequent to the initial seven provided to her on April 17, 2017. On June 23, 2017, Investigator Alberico received CyberTipline Report #20437297, which Google had previously submitted to NCMEC.³ On June 27, 2017, Investigator Alberico prepared a Douglas County search warrant affidavit, search warrant and non-disclosure order for the email account mringland69@gmail.com, associated with telephone number 402-***-0642. (Ex. 163 at pp. 1-2; Ex. 109-110). In obtaining the warrant, Investigator Alberico averred that Google "reviewed five hundred and two (502) files from the CyberTips submitted" and that she "only viewed files that were reviewed by Google . . . to confirm they depicted child pornography." (Ex. 109 at p. 7). On the same date, Investigator Alberico submitted the warrant electronically to Google through the Law Enforcement Request System ("LERS"). (Ex. 163 at p. 2).

On July 14, 2017, Investigator Alberico received the contents requested by the search warrant via FedEx from Google and saved the data to a digital case file. In reviewing the data, Investigator Alberico observed that email address mringland69@gmail.com had sent child erotica photographs and images of child pornography to the email address mringland65@gmail.com. (Ex. 163 at p. 2). On the same date, the South Dakota Bureau of Criminal Investigation ("SDBCI") contacted Investigator Alberico by email stating that it had received information from NCMEC that a case the SDBCI was working on was linked to Alberico's case. On July 19, 2017, Investigator Alberico received CyberTipline reports #21681475 and #22346425, which were originally assigned to the SDBCI.⁴ These CyberTipline reports listed the email address markringland65@gmail.com, with associated telephone 402-***-0902, and a secondary email

³ Investigator Alberico's affidavit dated August 7, 2017, submitted with an application for a search warrant in Douglas County states that the two images from the June 23, 2017, CyberTip (#20437297) were not viewed by Google. (Ex. 122 at p. 6).

⁴ Investigator Alberico averred that neither she nor Google reviewed these files. (Ex. 122 at p. 7).

address, mringland69@gmail.com. NCMEC traced several of the IP addresses associated with the uploaded files to Sprint PCS in the Omaha area, and Google provided the name "Mark Ringland" associated with the two email addresses. (Ex. 163 at p. 2). Pursuant to a subpoena served by Investigator Alberico on July 20, 2017, Sprint identified the subscriber of telephone number 402-***-0902 as Mark Ringland, residing at 1904 Pleasantview Ln, Bellevue, Nebraska 68005. On August 4, 2017, Investigator Alberico submitted a preservation letter to Google for the email account markringland65@gmail.com, associated telephone number 402-***-0902. (Ex. 163 at pp. 2-3).

On August 7, 2017, Investigator Alberico received nine more CyberTipline reports: #22968026, #22968382, #22968534, #23001904, #23002061, #2302151, #23002255, #23043174 and #23043630, all of which were associated with the email address markringland65@gmail.com. NCMEC traced some of the associated IP addresses to Sprint PCS, in the Omaha, Lincoln, and Grand Island, Nebraska areas. On the same date, Investigator Alberico prepared a Douglas County search warrant affidavit, search warrant, and non-disclosure order for the email accounts mringland65@gmail.com and markringland65@gmail.com, associated with telephone number 402-***-0902. (Ex. 122-123).

On August 14, 2017, Investigator Alberico received five additional CyberTipline reports, #23245909, #23274478, #23249764, #23249764 and #23068622, and on August 25, 2017, received six more, #23411893, #23488795, #23512952, #23545730, #23588762 and #233890937. All the reports were associated with email addresses markringland65@gmail.com and mringland69@gmail.com, and the telephone number 402-***-0902. (Ex. 163 at p. 4).

On August 18, 2017, Investigator Alberico received the search warrant response via LERS from Google and saved the data to a digital case file maintained at her office. (Ex. 163 at pp. 3-4). According to Investigator Alberico, several of the files contained images and/or videos of suspected child pornography and bestiality. (Ex. 124 at p. 10). Based on the information obtained during her investigation, on August 31, 2017, Investigator Alberico applied for a United States District Court search and seizure warrant affidavit, search warrant, and non-disclosure order for a cellular ping order for telephone number 402-***-0902, which was presented to and signed by a United States Magistrate Judge. (Ex. 124-125; Ex. 163 at p. 4).

⁵ Investigator Alberico averred that neither she nor Google reviewed these files. (Ex. 126 at p. 13).

Investigator Alberico located Mark Ringland in the Nebraska Criminal Justice System ("NCJIS"), which indicated that a black Ford Windstar SE sport van with Nebraska license plate number UZP192 was registered to Ringland in June 2017, and that as of August 2017, the vehicle's registration address was 16406 Taylor Street, Omaha, NE 68116. Nebraska Department of Labor records indicated that Ringland was employed by Merrick Machine Company, located in Alda, Nebraska, and by the temporary agency Essential Personnel Inc., based out of Grand Island Nebraska, with hub offices in Kearney, Nebraska and Denver, Colorado. (Ex. 163 at p. 3).

On September 1, 2017, Investigator Alberico prepared a United States District Court search warrant affidavit for Ringland's person and cellular telephone, phone number 402-***-0902, (Ex. 126-127), and a criminal complaint (Filing No. 1) and arrest warrant (Filing No. 3), which were signed by the undersigned magistrate judge. On the same date, members of the CETF, FBI, Nebraska State Patrol, and Douglas County Sheriff's Office implemented a search warrant at 16406 Taylor Street in Omaha, and arrested Ringland pursuant to the warrant. According to Investigator Alberico's report, Ringland was read his *Miranda* rights, which he waived, and consented to an interview. (Ex. 163 at p. 4). Investigator Alberico further indicated in her report that on September 5, 2017, Ringland made spontaneous statements to the US Marshals transporting him for his initial hearing. (Ex. 163 at pp. 4-5).

On September 5, 2017, Investigator Alberico received five more CyberTipline reports: #2360300, #23625155, #23660907, #23697631, and #23729375, which were associated with the email addresses markringland65@gmail.com and mringland69@gmail.com, and telephone number 402-***-0902. (Ex. 163 at p. 5). The Indictment was filed in this case on September 19, 2017. (Filing No. 20).

Defendant has filed the instant motions seeking suppression of all evidence seized during the investigation from the searches of his email accounts and any incriminatory statements he made after his arrest and during transportation to his initial appearance. (Filing Nos. 47, 49; TR. 55-56). Defendant argues that Google acted as a government agent when it searched his emails without a warrant and forwarded those contents to NCMEC, that NCMEC expanded upon Google's warrantless searches, and that the warrants obtained by Investigator Alberico were supported in substantial part by such warrantless searches. (Filing No. 47 at pp. 1-2). Defendant also seeks suppression of evidence and a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), arguing that the warrants were issued upon misleading applications that omitted material

information. Defendant separately argues that the applications in support of the warrants included information obtained by unconstitutional searches by government agents, and that no probable cause exists if that information was excluded from the warrant application. (Filing No. 49 at p. 1).

ANALYSIS

A. Defendant's Request for Franks Hearing

Defendant argues he is entitled to a *Franks* hearing both because material facts were intentionally omitted from the four search warrant applications and because the four search warrant applications included information and evidence that had been obtained through unconstitutional warrantless searches by Google and NCMEC. (Filing No. 49 at p. 3). A criminal defendant may request a hearing to challenge a search warrant on the ground that the supporting affidavit contains factual misrepresentations or omissions relevant to the probable cause determination. See *Franks*, 438 U.S. at 155-56. In order for a defendant to prevail on a request for a *Franks* hearing, the defendant must make a "substantial preliminary showing" that (1) the affiant "knowingly and intentionally" made reckless false statements or omissions and (2) if the false information is excised (or the omitted information is included), the affidavit no longer establishes probable cause. *United States v. Snyder*, 511 F.3d 813, 816 (8th Cir. 2008). "The requirement of a substantial preliminary showing is not lightly met[.]" *United States v. Arnold*, 725 F.3d 896, 898 (8th Cir. 2013)(quoting *United States v. Mathison*, 157 F.3d 541, 548 (8th Cir. 1998)).

Defendant first contends he is entitled to a *Franks* hearing because Investigator Alberico recklessly omitted from her warrant applications the fact that there were other geographic locations and IP addresses associated with the images in the CyberTipline reports. (Filing No. 50 at p. 2). Specifically, Defendant asserts that although the initial eight CyberTiplines supporting the June 27, 2017, warrant application contained two IP addresses that were traced to Sprint PCS in Omaha, several other IP addresses were associated with Des Moines, Chicago, Cleveland/Akron, the Quad Cities, and Minneapolis. (*Id.* at pp. 5-6). Defendant contends that the August 7, 2017, warrant application similarly omitted the material information that the two tips forwarded from the SDBCI were associated with IP addresses in Des Moines, Grand Island, and Chicago, and that the other nine tips reported IP addresses in Dannebrog, Nebraska, Watertown, South Dakota, Grand Island, and Raymore, Missouri. Defendant also states the August 7, 2017, application recklessly omitted the fact that, out of "the 11 CyberTips and 1113 files recounted in the application, NCMEC

identified only 22 as 'apparent child pornography' and labeled 1087 as 'uncategorized.'" (*Id.* at pp. 6-7). Likewise, Defendant asserts the August 31, 2017, ping warrant application omitted "dozens" of other IP addresses in ten other metropolitan areas and did not mention that "only 1.9% of those 1,109 files had been characterized as 'apparent child pornography' and 98.1% were deemed "uncategorized." (*Id.* at p. 7). Finally, Defendant argues the September 1, 2017, warrant application repeated all of the above omissions and also included "fruits of the receipts" from those warrants. (*Id.* at p. 8).

Upon review, the undersigned finds that Defendant has failed to demonstrate that the above omissions were material or necessary to a finding of probable cause. First, the omission of other IP addresses contained in the CyberTipline reports from Investigator Alberico's affidavits did not render the application materially misleading. Deputy Dishaw explained the difference between IP addresses assigned to a fixed tower as opposed to a mobile device. Deputy Dishaw testified that a fixed tower IP address can be geolocated to a certain area, whereas mobile service providers "have a limited number of IP addresses and cannot provide for every single customer of theirs an IP address," and therefore may need to assign an IP address from a different jurisdiction to a mobile user. (TR. 34-35; 53-54). Unlike a fixed tower IP address, therefore, a mobile IP address does not necessarily indicate the mobile user was accessing the internet in a certain geographic area; for example, a mobile user in Omaha may be assigned an IP address from Atlanta if one of the predetermined number of Omaha IP addresses were unavailable. (TR. 54). Moreover, as recognized by the government, Defendant is overstating the significance of the IP addresses to the finding of probable cause. (Filing No. 58 at p. 7). In this case, the CyberTipline reports identified email addresses and a phone number conclusively owned by Defendant which were associated with the files that triggered Google's reporting, making it very likely that a judge would have found sufficient probable cause to issue the warrant even had information about the other IP addresses been included in the affidavits. Therefore, the undersigned finds that any omitted information regarding the additional IP addresses would not have impacted the finding of probable cause in this case. See, e.g., United States v. Miller, No. 8:15CR172, 2015 WL 5824024, at *3 (D. Neb. Oct. 6, 2015)(rejecting similar argument that omission of other IP addresses from CyberTipline Reports rendered warrant application misleading).

Defendant's argument that the warrant applications recklessly omitted the breakdown of how many files were identified by NCMEC as "uncategorized" versus "apparent child

pornography" is also unavailing. Deputy Dishaw explained the differences in NCEMC designations of "apparent child pornography" versus "uncategorized." Deputy Dishaw testified that "apparent" child pornography files have been flagged by hash values, whereas "uncategorized" means the file was identified in manner other than by hash value; the fact that the file is labeled "uncategorized" does not exclude it from being child pornography. (TR. 52-53). More importantly, Investigator Alberico averred in her warrant application that she reviewed 502 images identified and viewed by Google, and confirmed they depicted child pornography. Accordingly, the fact that NCMEC designated other files as "uncategorized" has no bearing on the finding of probable cause, and as such, its omission from the warrant applications was not misleading.

Defendant's second argument in support of his request for a *Franks* hearing is tied to his separate motion to suppress (Filing No. 47); he contends that Google and NCMEC were state actors for purposes of the Fourth Amendment and that therefore their warrantless searches of his personal email and phone numbers were unconstitutional, and that such unconstitutionally obtained evidence impermissibly formed the "the entirety" of the probable cause supporting the warrants. (Filing No. 50 at p. 2). The undersigned will address Defendant's arguments in detail below, but in short, finds that the searches of Defendant's email and phone numbers were constitutional under the Fourth Amendment. Accordingly, the inclusion of such evidence in the warrant applications was not reckless or otherwise improper. Therefore, the undersigned recommends Defendant's request for a *Franks* hearing be denied.

B. Motion to Suppress Evidence

Defendant argues that his Fourth Amendment rights were violated when Google searched his email accounts without a warrant, and that all evidence obtained directly or indirectly from that search and the several subsequent searches should be suppressed.

The Fourth Amendment only applies to state action and its protection against unreasonable searches and seizures "is wholly inapplicable to a search or seizure . . . effected by a private individual not acting as an agent of the Government." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Defendant contends that Google effectively acted as a government agent under the Fourth Amendment when it undertook repeated searches of his email accounts and reported suspected child pornography to NCMEC. (Filing No. 48 at p. 3).

As previously discussed by the Eighth Circuit Court of Appeals, an internet service providers' fulfillment of child pornography reporting requirements under 18 U.S.C. § 2258A, standing alone, "does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography." *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013) (concluding AOL did not act as a government agent when it scanned a user's e-mail and reported apparent child pornography to NCMEC). Recognizing this Eighth Circuit precedent, Defendant asserts that *Riley v. California*, 134 S. Ct. 2473 (2014) has implicitly affected the decision in Stevenson because the Supreme Court "held that law enforcement needs a warrant before they can search the content of an individual's cell phone." (Filing No. 58 at p. 4). While the Supreme Court in *Riley* makes it clear that *law enforcement* generally needs to obtain a search warrant before searching data on cell phones, the decision in Riley does not address or discuss the propriety of a search by a private party such as Google. In this case, it is undisputed that Google is a private, for profit entity. Google's Senior Manager of Law Enforcement and Information Security submitted a sworn declaration indicating that Google implemented its "proprietary hashing technology" based on its "private, non-governmental interests" and based on its "strong business interest in enforcing our terms of service and ensuring that our services are free of illegal content, including[,] in particular[,] child sexual abuse material." (Filing No. 73-2 at p. 2). A private internet service provider's "voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent." Stevenson, 727 F.3d at 831. The undersigned therefore concludes Google simply complied with its statutory duty to report violations of child pornography laws and did not become a state actor by conducting its own searches of Defendant's email accounts to protect its own private, nongovernmental interests.

Defendant next argues that, even if the Court concludes that Google's searches fall under the private search doctrine, his Fourth Amendment rights were nevertheless violated because NCMEC expanded upon Google's private search. (Filing No. 48 at pp. 5-6). Defendant relies on *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), wherein the Tenth Circuit concluded that NCMEC is a government agent that violated the Fourth Amendment by expanding upon the scope of a private internet service provider's investigation without a warrant. In *Ackerman*, the undisputed facts established that NCMEC opened and viewed information other than the image flagged by AOL's hash values as known child pornography and had not been previously examined

by AOL. Therefore, the Tenth Circuit found that NCMEC exceeded, and did not merely repeat, the internet service provider's private search in violation of the Fourth Amendment. See *Ackerman*, 831 F.3d at 1306-07; see *United States v. Boyer*, 914 F.2d 144, 146 (8th Cir. 1990)("[T]he government may not exceed the scope of the private search unless it has the right to make an independent search[.]"). Conversely, in *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018), the Fifth Circuit found that law enforcement did not violate the Fourth Amendment because the investigator "reviewed only those files whose hash values corresponded to the hash values of known child pornography images" as ascertained by the internet service provider's system. *Id.* at 640.

In this case, the undersigned finds that the evidence does not support Defendant's assertion that NCMEC viewed more files than those identified and reviewed by Google. Therefore, this case is more like *Reddick* than *Ackerman*. Between March 20, 2017 and April 18, 2017, Google identified and reported 1,216 instances of suspected child pornography linked to email accounts owned by Defendant to NCMEC. Google reported having viewed 502 of these files. In her affidavit, Investigator Alberico attested that she viewed the same 502 images that has been reviewed by Google. (Ex. 109 at p. 7). The evidence did not establish that NCMEC reviewed more files than those reviewed by Google, and it is clear that Investigator Alberico's review did not exceed the scope of the private search done by Google. Accordingly, the Fourth Amendment is not implicated, and the undersigned therefore recommends that Defendant's motion to suppress be denied.

Finally, Defendant argues that the good faith exception does not apply in this case. (Filing No. 70 at p. 39). An exception to the exclusionary rule applies where officers rely on a warrant in good faith. *United States v. Hessman*, 369 F.3d 1016, 1019 (8th Cir. 2004). "In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause." *United States v. Leon*, 468 U.S. 897, 920 (1984). Even assuming that the warrantless searches performed by Google or NCMEC were found to be violative of the Fourth Amendment, the undersigned finds no evidence of deliberate, reckless, or grossly negligent conduct by law enforcement in relying on the warrants prepared based upon that information. When Investigator Alberio applied for an acquired the search warrants, she had no reason to believe that NCMEC had provided her with

information procured in violation of Defendant's Fourth Amendment rights. The evidence reflects that Investigator Alberico submitted her applications for warrants based on her personal review of the 502 images she knew to have already been reviewed by Google, which formed the basis of the probable cause upon which the applications relied. Accordingly, the undersigned concludes that law enforcement acted reasonably and in good faith in relying on the warrants issued in this case.

Upon consideration,

IT IS HEREBY RECOMMENDED to Chief United States District Court Judge Laurie Smith Camp that:

- 1. Defendant's Motion to Suppress Evidence and Statements and Request for Evidentiary Hearing (Filing No. 47) be denied, and
- 2. Defendant's Motion to Suppress, Application for *Franks* Hearing, and Request for Evidentiary Hearing and Oral Argument (Filing No. 49) be denied.

Dated this 19th day of October, 2018.

BY THE COURT:

s/ Michael D. Nelson United States Magistrate Judge

ADMONITION

Pursuant to NECrimR 59.2, any objection to this Findings and Recommendation shall be filed with the Clerk of the Court within fourteen (14) days after being served with a copy of this Findings and Recommendation. Failure to timely object may constitute a waiver of any such objection. The brief in support of any objection shall be filed at the time of filing such objection. Failure to file a brief in support of any objection may be deemed an abandonment of the objection.